REMARKS

Claims 1, 9, 15-16, and 21 are amended, no claims are canceled, and claim 25 is added; as a result, claims 1-25 are now pending in this application.

No new matter has been added through the amendments to claims 1, 9, 15-16, and 21. Support for the amendments to claims 1, 9, 15-16, and 21 may be found throughout the specification, for example but not limited to, the specification at page 2, line 32 through page 3, line 5.

No new matter has been added through new claim 25. Support for new claims 25 may be found throughout the specification, for example but not limited to the specification at page 2, line 32 through page 3, line 5, at page 6, lines 15 through page 8, lines 23 and in claim 1 as orginally filed in the application.

§*103 Rejection of the Claims*

Claims 1-22

Claims 1-22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Aucsmith (U.S. 5,712,800) in view of Marino et al. (U.S. 6,026,165). Applicants respectfully traverse the rejection of claims 1-22.

Applicants maintain each of the arguments provided in Applicants' previous response[1] with regards to the Office Action failing to provide a showing of a motivation or suggestion in the prior art for forming the proposed combination of Aucsmith with Marino et al. In reply to these arguments, the currently pending Office Action merely states,[2]

> In this case, Aucsmith and Marino both deal with transmitters and receivers selecting transmitting/receiving messages intended for each other without comprising security, i.e. easily adaptable(multiple device keys).

However, these statements appear to be a general description of features of the Aucsmith and Marino et al. patents, but fail to provide any evidence of why one of ordinary skill in the art would have *a motivation or suggestion* to make the proposed combination. Also, the Office

[1] See Applicants' response mailed June 6, 2006 at page 12 in reply to the Office Action mailed April 7, 2006 in this application.
[2] See the currently pending Office Action at page 3.

Action fails to provide support for, or any evidence of record, to support the statement, "easily adaptable(multiple device keys)." Without such support, these statements, and the statements made in the previous Office Action[3] fail to meet the requirements of providing a motivation or suggestion for making the proposed combination of Aucsmith and Marino et al. Further, none of these statements as provided in the Office Action show the desirability[4] of making the proposed combination of Aucsmith and Marino et al. Thus, the Office Action appears to be basing the proposed combination of Aucsmith and Marino et al. on impermissible hindsight[5] using Applicants' claimed subject matter as a blueprint.

For at least the reasons stated above, the Office Action fails to meet its required burden for establishing a *prima facie* case of obviousness with respect to claims 1-22.

Even if the propose combination of Aucsmith an Marino et al. could be formed (which Applicants expressly do not admit that it could), the proposed combination of Aucsmith and Marion et al. fails to teach or suggest all of the subject matter included in claims 1-22. For example, claim 1 as now amended includes,

> A transmission system for providing conditional access to transmitted data; the system including a transmitter and a plurality of receivers coupled via a network;
>
> the transmitter including means for transmitting:
>
> to all receivers same the same data encrypted under control of a same authorization key; and
>
> to all receivers a same key block with a plurality of entries, wherein each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key, and
>
> each of the receivers being associated with a corresponding set of a plurality of device keys, **wherein at least two of the receivers are associated with sets that comprise at least one corresponding device key**, each of the receivers including
>
> means for receiving the key block and the encrypted data;

---

[3] See the Office action mailed April 7, 2006 in this application.

[4] The fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990); MPEP § 2143.01.

[5] The Examiner must avoid hindsight. *In re Bond* at 834.

> **a first decryptor for retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key; and**
> a second decryptor for decrypting the encrypted data under control of the authorization key.
> (Emphasis added).

Thus, claim 1 includes, "each of the receivers being associated with a corresponding set of a plurality of device keys, wherein at least two of the receivers are associated with sets that comprise at least one corresponding device key." Further, claim 1 also includes, "a first decryptor for retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key." At least this subject matter is not taught or suggested by the proposed combination of Aucsmith and Marino et al.

In contrast to claim 1, Aucsmith concerns a communication system comprising a transmitter system for distributing keys to a plurality of receivers. The transmitter system of Aucsmith utilizes a private key and a prime number associated with each receiver I to generate a unique value X. The value X is broadcast to all receivers i and each receiver uses both the prime number and the private key to arrive at a master key (see abstract).

In particular, Figure 3 of Aucsmith illustrates a communication network 40 coupling a transmitter unit 10 with a plurality of receiver units 20-38. Each receiver 20-38 of the network 40 has an associated private key and a prime number and this key and prime are used to decode a master encryption key that is broadcast as a single value in coded form to all units 28-30 (column 6, line 55 – column 7, line 10).

The transmitter 10 in Aucsmith generates a master key K. The key K is used to decrypt an encoded message C. The transmitter encodes this key K using the private keys k(i) of all receivers in a group G. Each receiver is further associated with a prime number p(i). The private keys k(i) and the prime number p(i) are both used to obtain a value X. X is broadcast over the communication network 40. At the receivers, the masker key K can be obtained using both k(i) and p(i) (column 8, line 56 – column 9, line 29).

Claim 1 differs substantially from what is described in Aucsmith. In particular, the subject matter as included in claim 1 differs from Aucsmith by at least the following features:

- a key block, wherein some of the entries contain a representation of the authorization key, encrypted with the associated device key; and
- retrieving of the authorization key by taking one of the device keys of a set of device keys.

It is noted that in Aucsmith, the master key K is obtained at the receivers using both the private key k(i) and the prime number p(i), which 'keys' were both utilized for encrypting the master key K at the transmitter. This becomes clear from the entire disclosure, in particular column 3, lines 20, 21; column 3, line 67- column 4, line 1; column 9, lines 27, 28; column 11, lines 3-20.

In contrast, whereas each receiver according claim 1 is associated with a set of device keys, the receiver is capable of retrieving the authorization key by taking only a single key from this set for the decrypting of the entries of the key block. It is this aspect that increases the flexibility in the updating of the authorization key according to the invention.

Furthermore, in Aucsmith, each receiver i is associated with a private key k(i) and a prime number p(i). From the index i, it is clear that the private keys and prime numbers are different for each receiver. In contrast, the subject matter of for example 1, requires that at least one of the device keys of the set corresponds to a device key of another receiver in the system. This subject matter as included in claim 1 provides for a reduced size of the key block which in turn increases the security of the transmission system as it facilitates a more frequent transmission of the key block over the network.

Thus there is no teaching or suggestion in Aucsmith of "each of the receivers being associated with a corresponding set of a plurality of device keys, wherein at least two of the receivers are associated with sets that comprise at least one corresponding device key," and no teaching or suggestion in Aucsmith of "a first decryptor for retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key," as is included in claim 1.

For at least the reasons stated above, Aucsmith fails to teach or suggest the subject matter included in claim 1. The addition document of Marino et al. also fails to teach or suggest the subject matter included in claim 1 and missing from Aucsmith.

In contrast to claim 1, Marino et al. discloses a secure communication system comprising a plurality of transmitters 2a, 2b and 2c wirelessly connected with a single receiving station 4 (column 6, lines 21-32; Figure 1). The encoder 7 of a transmitter 2 transmits a data field 28, a device ID field 30, a sequence number field 32 and a CRC field 34 to the receiver 6 of a receiving station 4 (column 7, lines 14-17). The data field is encrypted by a key and decrypted by a corresponding key stored in the receiver (column 7, lines 20-25). The device ID, which is not encrypted, is used by the receiver 6 to fetch the stored key from a memory table at the receiver (column 7, lines 32-35 and lines 58-61). The sequence number is sent in encrypted format and is used by the receiver 6 to ensure that the communication is received from an authorized transmitter (column 7, lines 35-41).

In further contrast to claim 1, Marino et al. discloses a system with only a single receiving unit. Furthermore, it is noted that Marino does not disclose a key block that is transmitted and comprise entries that contain a representation of the authorization key. The authorization key is a key that controls the decryption of the encrypted data received by the receivers. The encrypted data block 28 of Marino is decrypted by using keys stored in a memory table 42 (column 7, lines 58-61). Apart from the fact that Marino only discloses a single receiver, Marino fails to disclose or suggest that a device key, let alone a set of such keys, is associated with the receiving unit 4. As a consequence of the three preceding distinguishing features, Marino by definition does not disclose the feature of retrieving of the authorization key by taking one of the device keys of a set of device keys, as included in claim 1.

Thus, there is no teaching or suggestion in the proposed combination of Aucsmith and Marion et al. of "each of the receivers being associated with a corresponding set of a plurality of device keys, wherein at least two of the receivers are associated with sets that comprise at least one corresponding device key," and no teaching or suggestion in the proposed combination of Aucsmith and Marion et al. of "a first decryptor for retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated

with the receiver and decrypting at least one entry of the key block that is associated with the single one device key," as is included in claim 1.

Therefore, the proposed combination of Aucsmith and Marino et al. fails to teach or suggest all of the subject matter included in claim 1, and so claim 1 is not obvious in view of the proposed combination of Aucsmith and Marino et al.

In further examples of claimed subject matter included in claims 1-22 and not taught or suggested by the proposed combination of Aucsmith and Marion et al.:

Independent claim 9 as now amended includes:

> A transmission system for providing conditional access to transmitted data including:
>
> a transmitter and a plurality of receivers coupled via a network;
>
> the transmitter configured to transmit a same data stream encrypted under control of a same authorization key to all receivers and to all receivers a same key block with a plurality of entries, wherein each entry is associated with a different device key, at least one of the entries containing a representation of the authorization key encrypted with the associated device key, and
>
> each of the receivers being associated with a corresponding set of a plurality of device keys and being configured to receive the key block and the encrypted data, with a first decryptor for retrieving the authorization key by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key and a second decryptor for decrypting the data under control of the authorization key.

Independent claim 21 as now amended includes:

> A method for providing conditional access to transmitted data over a network including a transmitter and a plurality of receivers, each of said receivers being associated with a corresponding set of a plurality of device keys, said method comprising the steps of:
>
> transmitting the same data to all receivers, wherein said same data is encrypted under control of a same authorization key;
>
> transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries

containing a representation of the authorization key encrypted with the associated device key;

receiving at each receiver the key block and the encrypted data, wherein each receiver is associated with a set of a plurality of device keys and wherein at least one of the device keys of the set corresponds with a device key of a set associated with another receiver in the system;

retrieving the authorization key at one or more of said plurality of receivers by taking a single one of the device keys from the corresponding set of a plurality of device keys associated with the receiver and decrypting at least one entry of the key block that is associated with the single one device key; and

decrypting the data at said one or more of said plurality of receivers under control of the authorization key.

For reasons analogous to those stated above with respect to claim 1, the proposed combination of Aucsmith and Marino et al. also fails to teach or suggest all of the claimed subject matter included in claim 9 and in claim 15, and so claims 9 and 21 are not obvious in view of the proposed combination of Aucsmith and Marino et al.

Further, claims 2-5, 7-8 and 19-20 depend from claim 1, and so include all of the subject matter included in claim 1, and more, Claims 10-13 and 15-18 depend from claim 9, and so include all of the subject matter included in claim 9, and more. Claim 22 depends from claim 21, and so includes all of the subject matter included in claim 21, and more. For at least the reasons stated above with respect to claims 1, 9, and 21, the proposed combination of Aucsmith and Marino et al. fails to teach or suggest the subject matters as included in each of dependent claims 2-5, 7-8, 10-13, 15-20, and 22, and so claims 2-5, 7-8, 10-13, 15-20, and 22 are not obvious in view of the proposed combination of Aucsmith and Mario et al.

Applicants respectfully request withdraw of the rejection, and reconsideration and allowance of claims 1-22.

Claims 3-4 and 11-12

Claims 3-4 and 11-12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Aucsmith (U.S. 5,712,800) in view of Marino et al. (U.S. 6,026,165) and further in view of Lotspiech (U.S. 6,118,873). Applicants respectfully traverse the rejection of claims 3-4 and 11-12.

Applicants maintain for at least the reasons stated above with respect to the proposed combinational of Aucsmith and Marino et al. that the Office Action has not met the requirements for forming the proposed combination of Aucsmith, Mario et al., and Lotspiech in rejecting claims 3-4 and 11-12. By failing to meet these requirements, the Office Action fails to establish a *prima facie* case of obviousness with respect to claim 3-4 and 11-12.

Further, Applicants believe they have established that the proposed combination of Aucsmith and Marion et al. fails to teach or suggest all of the subject matter included in claim 1, and all of the subject matter included in claim 9. Claims 3-4 depend from claim 1, and so include all of the subject matter included in claim 1, and more. Claims 11-12 depend from claim 9, and so include all of the subject matter included in claim 9, and more.

For at least the reasons stated above with respect to claims 1 and 9, the proposed combination of Aucsmith and Mario et al. fails to teach or suggest all of the subject mater included in claims 3-4 and 11-12. Applicants' representatives fail to find in, and the Office Action fails to point out in Lotspiech, a teaching or suggestion of the subject matter included in claims 3-4 and claim 11-12 and missing from the proposed combination of Aucsmith and Marino et al. Thus, the proposed combination of Aucsmith, Marino et al., and Lotspiech fails to teach or suggest the subject matter included in claims 3-4 and 11-12, and so claim 3-4 and 11-12 are not obvious in view of the proposed combination of Aucsmith, Mario et al., and Lotspiech.

Applicants respectfully request withdraw of the rejection, and reconsideration and allowance of claims 3-4 and 11-12.

Claims 23 and 24

Claims 23 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Aucsmith (U.S. 5,712,800) in view of Marino et al. (U.S. 6,026,165) and further in view of Traw et al. (U.S. 6,542,610). Applicants respectfully traverse the rejection of claims 23 and 24.

Applicants maintain for at least the reasons stated above with respect to the proposed combinational of Aucsmith and Marino et al. that the Office Action has not met the requirements for forming the proposed combination of Aucsmith, Mario et al., and Traw et al. in rejecting claims 23 and 24. By failing to meet these requirements, the Office Action fails to establish a *prima facie* case of obviousness with respect to claim 23 and 24.

Further, Applicants believe they have established that the proposed combination of Aucsmith and Marion et al. fails to teach or suggest all of the subject matter included in claim 21. Claims 23 and 24 depend from claim 21, and so include all of the subject matter included in claim 21, and more

For at least the reasons stated above with respect to claim 21, the proposed combination of Aucsmith and Mario et al. fails to teach or suggest all of the subject mater included in claims 23 and 24. Applicants' representatives fail to find in, and the Office Action fails to point out in Traw et al., a teaching or suggestion of the subject matter included in claims 23 and 24 and missing from the proposed combination of Aucsmith and Marino et al. Thus, the proposed combination of Aucsmith, Marino et al., and Traw et al. fails to teach or suggest the subject matter included in claims 23 and 24, and so claim 23 and 24 are not obvious in view of the proposed combination of Aucsmith, Mario et al, and Traw et al.

Applicants respectfully request withdraw of the rejection, and reconsideration and allowance of claims 23-24.

Allowable Subject Matter

Claims 5 and 13 were objected to as being dependent upon a rejected base claim, but were indicated to be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Applicants acknowledge the indication of allowability of claims 5 and 13 if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicants have not amended claims 5 and 13 to place them in independent form at this time. Pursuant to arguments presented above, Applicants respectfully submit that these claims are in condition for allowance.

Reservation of Rights

Applicants do not admit that references cited under 35 U.S.C. §§ 102(a), 102(e), 103/102(a), or 103/102(e) are prior art, and reserves the right to swear behind them at a later date. Arguments presented to distinguish such references should not be construed as admissions that the references are prior art.

CONCLUSION

Applicants respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicants' attorney at 612-371-2132 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

BARTHOLOMEUS JOHANNES VAN RIJNSOEVER ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-278-4042

Date DECEMBER 15/2006 By Robt B Madden

Robert B. Madden
Reg. No. 57,521

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 15 day of December 2006.

Dawn R. Shaw — Name

/Dawn R. Shaw/ — Signature